

# The reciprocity conjecture of Khare and Wintenberger

Romyar T. Sharifi\*

## Abstract

We prove a strengthening of the “reciprocity conjecture” of Khare and Wintenberger. The input to the original conjecture is an odd prime  $p$ , a CM number field  $F$  containing the  $p$ th roots of unity, and a pair  $(\mathfrak{q}_1, \mathfrak{q}_2)$  of primes of the maximal totally real subfield  $F^+$  of  $F$  that are inert in the cyclotomic  $\mathbf{Z}_p$ -extension  $F_\infty^+/F^+$ . In analogy to a statement about generalized Jacobians of curves, the conjecture asserts the equality of two procyclic subgroups of the Galois group of the maximal pro- $p$  extension  $\mathcal{M}$  of  $F_\infty^+$  that is unramified outside  $p$  and abelian over  $F^+$ . The first is the intersection with  $\text{Gal}(\mathcal{M}/F_\infty^+)$  of the closed subgroup of  $\text{Gal}(\mathcal{M}/F^+)$  generated by the Frobenius elements of  $\mathfrak{q}_1$  and  $\mathfrak{q}_2$ . The second is generated by the class of an exact sequence defining the minus part of the  $p$ -part of the ray class group of  $F_\infty$  of conductor  $\mathfrak{q}_1\mathfrak{q}_2$ .

## 1 Introduction

The goal of this paper is to prove the reciprocity conjecture of Khare and Wintenberger, as found in [KW, Conjecture 5.5]. The conjecture as originally stated asserts the equality of two procyclic subgroups of the Galois group of the maximal abelian pro- $p$  extension of a totally real field. These subgroups fix the cyclotomic  $\mathbf{Z}_p$ -extension, hence are conjecturally finite by Leopoldt’s conjecture. In fact, as we shall shortly explain, the reciprocity conjecture may be used to give an equivalent formulation of Leopoldt’s conjecture in terms of ray class groups. In this introduction, we give the original formulation and a slight extension of the conjecture and recall the motivation for the conjecture from [KW]. Let us begin straightaway with the formulation.

---

\*Department of Mathematics, University of Arizona, P.O. Box 210089, Tucson, AZ 85721, USA, sharifi@math.arizona.edu

Let  $p$  be an odd prime, let  $F$  be a CM field containing  $\mu_p$ , and let  $F^+$  be its maximal totally real subfield. Let  $F_\infty$  and  $F_\infty^+$  denote the cyclotomic  $\mathbf{Z}_p$ -extensions of these respective fields, and let  $\Gamma = \text{Gal}(F_\infty/F)$ . Let  $Q^+ = \{\mathfrak{q}_1, \mathfrak{q}_2\}$  be a set of two distinct finite primes of  $F^+$  not lying over  $p$ , and suppose that these primes remain inert in  $F_\infty^+$ . Let  $\mathcal{M}$  (resp.,  $\mathcal{M}_\infty$ ) denote the maximal abelian pro- $p$  unramified outside  $p$  extension of  $F^+$  (resp.,  $F_\infty^+$ ).

Let  $\varphi_i$  denote the Frobenius element in  $\text{Gal}(\mathcal{M}/F^+)$  attached to  $\mathfrak{q}_i$  for  $i \in \{1, 2\}$ . Each  $\varphi_i$  restricts nontrivially to  $F_\infty^+$ , so the subgroup  $\overline{\langle \varphi_1, \varphi_2 \rangle}$  topologically generated by  $\varphi_1$  and  $\varphi_2$  has a procyclic intersection with the kernel of this restriction map. This provides the first of the two procyclic subgroups  $M_Q$  and  $N_Q$  of  $\text{Gal}(\mathcal{M}/F_\infty^+)$  that are the subject of the reciprocity conjecture.

**Definition 1.1.** The Frobenius line  $M_Q$  is the intersection  $\overline{\langle \varphi_1, \varphi_2 \rangle} \cap \text{Gal}(\mathcal{M}/F_\infty^+)$ .

Let  $A_\infty$  and  $A_{\infty, \mathfrak{q}}$  denote the  $p$ -parts of the class group of  $F_\infty$  and the ray class group of conductor  $\mathfrak{q}_1 \mathfrak{q}_2$  of  $F_\infty$ , respectively. We denote the minus parts of these groups, on which complex conjugation acts by  $-1$ , with a superscript “ $-$ ”. The definition of the ray class group gives rise to an exact sequence of  $\mathbf{Z}_p[[\Gamma]]$ -modules

$$0 \rightarrow \mu_{p^\infty} \rightarrow A_{\infty, \mathfrak{q}}^- \rightarrow A_\infty^- \rightarrow 0, \quad (1.1)$$

the subgroup  $\mu_{p^\infty}$  being identified with the  $p$ -power torsion in the residue field of  $F_\infty^+$  for  $\mathfrak{q}_1$ . (Here, that the  $\mathfrak{q}_i$  are inert allows the sequence to have this simple form, given a choice between the two primes.) As shown by Iwasawa [I1, p. 75], Kummer theory provides a canonical isomorphism between  $\text{Hom}(A_\infty^-, \mu_{p^\infty})$  and  $\text{Gal}(\mathcal{M}_\infty/F_\infty^+)$ . The  $\Gamma$ -coinvariants of the latter group are canonically isomorphic to  $\text{Gal}(\mathcal{M}/F_\infty^+)$  and non-canonically, i.e., up to a choice of generator of  $\Gamma$ , isomorphic to the continuous cohomology group  $H^1(\Gamma, \text{Gal}(\mathcal{M}_\infty/F_\infty^+))$ . The next object was not named in [KW], so we give it a name to put in on a equal footing with the Frobenius line.

**Definition 1.2.** The ray class line  $N_Q$  is the topological subgroup of  $\text{Gal}(\mathcal{M}/F_\infty^+)$  generated by the image of the class of the extension (1.1) of  $\mathbf{Z}_p[[\Gamma]]$ -modules in

$$H^1(\Gamma, \text{Gal}(\mathcal{M}_\infty/F_\infty^+)) \cong \text{Gal}(\mathcal{M}/F_\infty^+). \quad (1.2)$$

We remark that while the class of (1.1) depends up to sign on a choice of  $\mathfrak{q}_1$  over  $\mathfrak{q}_2$  and a choice of generator of  $\Gamma$ , the ray class line  $N_Q$  does not. We may now state the reciprocity conjecture of Khare and Wintenberger. Despite its name, we will not employ class field theory in our approach to it.

**Conjecture 1.3** (Khare-Wintenberger). *The Frobenius line  $M_Q$  and the ray class line  $N_Q$  are equal.*

Let us briefly consider the connection with Leopoldt's conjecture for totally real fields [L], which provides something of an impetus for the investigation of the relationship between  $M_Q$  and  $N_Q$ . We recall the statement for an arbitrary number field.

**Conjecture 1.4** (Leopoldt). *Let  $E$  be a number field. Then the topological closure of the embedding of the units  $\mathcal{O}_E^\times$  of  $E$  in the direct product of the completions  $E_v^\times$  at the primes  $v$  of  $E$  lying over  $p$  has  $\mathbf{Z}_p$ -rank equal to the rank of  $\mathcal{O}_E^\times$  as an abelian group.*

The rank of  $\mathcal{O}_E^\times$  in Leopoldt's conjecture is always at least the  $\mathbf{Z}_p$ -rank of the topological closure, but Leopoldt's conjecture asserts that it is never less. As Iwasawa pointed out in [I2, Section 2.3], Leopoldt's conjecture for a totally real number field is equivalent to the statement that its maximal abelian, unramified outside  $p$ , pro- $p$  extension is a finite extension of its cyclotomic  $\mathbf{Z}_p$ -extension.

It is, of course, sufficient to prove Leopoldt's conjecture for totally real fields for fields  $F^+$  of the sort we consider, since any totally real field sits inside of such an  $F^+$ . And, as we have just noted, Leopoldt's conjecture for  $F^+$  is equivalent to the statement that  $\text{Gal}(\mathcal{M}/F_\infty^+)$  is finite. The following result of Khare and Wintenberger [KW, Corollary 6.5], which is a consequence of the Čebotarev density theorem, tells us that Leopoldt's conjecture for  $F^+$  and  $p$  is equivalent to the finiteness of the ray class lines  $N_Q$  for all pairs  $(\mathfrak{q}_1, \mathfrak{q}_2)$ .

**Theorem 1.5** (Khare-Wintenberger). *Leopoldt's conjecture holds for  $F^+$  and  $p$  if and only if the Frobenius line  $M_Q$  is a finite group for every pair  $(\mathfrak{q}_1, \mathfrak{q}_2)$  of primes of  $F^+$  not lying over  $p$  and inert in  $F_\infty^+/F^+$ .*

In their work, Khare and Wintenberger explain that the reciprocity conjecture is a natural analogue in Iwasawa theory of a statement one can make for the generalized Jacobian  $J_{P_1, P_2}$  of the singular curve obtained by identifying two rational points  $P_1, P_2$  of a smooth projective curve  $X$  over a field  $k$  [KW, Section 5.3]. That is, the Tate module  $T_\ell(J_{P_1, P_2})$  of the generalized Jacobian for a prime  $\ell \neq \text{char } k$  fits in an exact sequence of  $\mathbf{Z}_\ell[[G_k]]$ -modules

$$0 \rightarrow \mathbf{Z}_\ell(1) \rightarrow T_\ell(J_{P_1, P_2}) \rightarrow T_\ell(J) \rightarrow 0,$$

where  $J$  denotes the Jacobian of  $X$  and  $G_k$  is the absolute Galois group of  $k$ , and where the map from  $\mathbf{Z}_\ell(1)$  to the Tate module is given by fixing a choice of  $P_1$  among the two primes. Using Weil duality, the class of this extension may be viewed as lying in the

continuous cohomology group  $H^1(G_k, T_\ell(J))$ , and this class is identified via Kummer theory with the class of the divisor  $(P_2) - (P_1)$  in the  $\ell$ -part of  $J(k)$ .

We remark that the latter statement is a bit stronger than what would be analogous to the reciprocity conjecture, which asserts an equality of subgroups, rather than elements. However, this may be fixed. We make several choices corresponding to a choice of  $\mathfrak{q}_1$  over  $\mathfrak{q}_2$ . Let  $m_Q$  denote the unique element of  $M_Q$  that is  $\varphi_1 \varphi_2^j$  for some  $j \in \mathbf{Z}_p^\times$ . The  $\mu_{p^\infty}$  found in (1.1) is more canonically written as  $(\mu_{p^\infty} \oplus \mu_{p^\infty})/\mu_{p^\infty}$ , with the  $i$ th coordinate corresponding to the  $p$ -power roots of unity in the residue field of  $F_\infty^+$  at  $\mathfrak{q}_i$  for  $i \in \{1, 2\}$ . We consider the isomorphism taking the image of  $(\alpha, \beta)$  to  $\alpha\beta^{-1}$ . Finally, evaluation at a choice of generator of  $\Gamma$  followed by restriction provides the isomorphism (1.2), and we may take the restriction of  $\varphi_1$  as a canonical choice. With these consistent choices, the class of (1.1) defines a generator  $n_Q$  of  $N_Q$ . A refined form of the reciprocity conjecture may then be stated. As we shall prove it, we state it as a theorem.

**Theorem 1.6.** *The generators  $m_Q$  and  $n_Q$  of the Frobenius line and the ray class line, respectively, are the negatives of each other.*

In fact, we will prove in Theorem 2.1 a strengthening of this conjecture in which we allow  $Q^+$  to be an arbitrary finite set of finite primes of  $F^+$  not lying over  $p$  that are no longer assumed to be inert in the extension  $F_\infty^+/F^+$ .

The structure of this paper is simple. In Section 2, we reformulate and generalize the statement of the conjecture. In Section 3, we provide the proof of our more general statement. Our proof will use little beyond standard facts regarding Galois cohomology and Kummer theory for number fields, hence the paucity of references.

*Acknowledgments.* The author thanks Chandreshekhar Khare for introducing him to the reciprocity conjecture and for his helpful comments on drafts of this work. He was supported in part during the preparation of this work by NSF award DMS-0901526.

## 2 The conjecture

In this section, we start afresh and introduce the strengthening of the reciprocity conjecture that we intend to prove. This requires a reasonable amount of notation and set-up, so let us embark upon the task.

Let  $p$  be an odd prime number. Fix a CM number field  $F$  containing  $\mu_p$ , and let  $F^+$  be its maximal totally real subfield. Let  $Q^+$  be a fixed finite set of finite primes of  $F^+$  not lying over  $p$  and  $Q$  the set of primes of  $F$  lying above them. Let  $\mathfrak{q}$  denote the

product of the primes in  $Q$ . More generally, for any algebraic extension  $E$  of  $F^+$ , we will let  $Q_E$  denote the set of primes of  $E$  lying over those in  $Q^+$ . If  $E$  is a number field, we let  $\mathfrak{q}_E$  denote the product of the primes in  $Q_E$ , and we let  $E_w$  denote the completion of  $E$  at  $w \in Q_E$ .

We let  $F_\infty$  denote the cyclotomic  $\mathbf{Z}_p$ -extension of  $F$  and  $F_\infty^+$  its maximal totally real subfield. The (finite) sets of primes above  $Q^+$  in  $F_\infty^+$  and  $F_\infty$  will be denoted  $Q_\infty^+$  and  $Q_\infty$ , respectively. Let  $\mathfrak{q}_\infty$  denote the product of the primes in  $Q_\infty$ . Set  $\Gamma = \text{Gal}(F_\infty/F)$  and  $\Lambda = \mathbf{Z}_p[[\Gamma]]$ .

We let  $\Omega$  denote the maximal unramified outside the primes over  $p$  (or,  $p$ -ramified) extension of  $F$ , and we set  $G = \text{Gal}(\Omega/F)$  and  $H = \text{Gal}(\Omega/F_\infty)$ . As usual, for a  $\mathbf{Z}[\text{Gal}(F_\infty/F_\infty^+)]$ -module  $B$ , we let

$$B^\pm = \{b \in B \mid s(b) = \pm b\}$$

for the generator  $s$  of  $\text{Gal}(F_\infty/F_\infty^+)$ , which is to say complex conjugation.

Let  $\mathfrak{X}$  denote the Galois group of the maximal  $p$ -ramified abelian pro- $p$  extension of  $F$ . Let  $\mathcal{O}$  denote the ring of integers of  $F$ . Let  $\text{Cl}$  denote the class group of  $\mathcal{O}$  and  $A$  its  $p$ -part. Similarly, let  $\text{Cl}_{\mathfrak{q}}$  denote the ray class group of conductor  $\mathfrak{q}$  and  $A_{\mathfrak{q}}$  its  $p$ -part. The corresponding objects over  $F_\infty$  will be denoted with a subscript  $\infty$ . Note that  $\mathfrak{X}_\infty$  is a finitely generated (compact)  $\Lambda$ -module, while  $A_\infty$  and  $A_{\infty, \mathfrak{q}}$  are cofinitely generated (discrete)  $\Lambda$ -modules.

For each  $v \in Q^+$ , let  $D_v$  denote the decomposition group at  $v$  in  $\mathfrak{X}^+$ , and let  $\Gamma_v$  denote the decomposition group at  $v$  in  $\Gamma$ . Note that  $\Gamma_v$  is nontrivial as no prime ideal splits completely in the cyclotomic  $\mathbf{Z}_p$ -extension of a number field. As  $D_v$  is procyclic, this forces the restriction map  $D_v \rightarrow \Gamma_v$  to be an isomorphism. The direct sum of the inverses  $\Gamma_v \rightarrow D_v$  of the restriction isomorphisms composed with the inclusion maps  $D_v \rightarrow \mathfrak{X}^+$  yields a homomorphism

$$\delta: \bigoplus_{v \in Q^+} \Gamma_v \rightarrow \mathfrak{X}^+.$$

Note that the group  $(\mathfrak{X}_\infty^+)_{\Gamma}$  of  $\Gamma$ -coinvariants is canonically isomorphic to the Galois group of the largest subextension of the maximal  $p$ -ramified abelian pro- $p$  extension of  $F_\infty^+$  that is actually abelian over  $F^+$ . We therefore have a short exact sequence of abelian Galois groups

$$0 \rightarrow (\mathfrak{X}_\infty^+)_{\Gamma} \rightarrow \mathfrak{X}^+ \rightarrow \Gamma \rightarrow 0.$$

We define  $M_Q$  to be the image of the induced map  $\delta^0$  in the commutative diagram

$$\begin{array}{ccc}
 0 & & 0 \\
 \downarrow & & \downarrow \\
 \bigoplus_{Q^+}^0 \Gamma_v & \xrightarrow{-\delta^0} & (\mathfrak{X}_\infty^+)_\Gamma \\
 \downarrow & & \downarrow \\
 \bigoplus_{Q^+} \Gamma_v & \xrightarrow{\delta} & \mathfrak{X}^+ \\
 \downarrow & & \downarrow \\
 \Gamma & \xlongequal{\quad} & \Gamma \\
 & & \downarrow \\
 & & 0
 \end{array} \tag{2.1}$$

with exact columns, where  $\bigoplus^0$  denotes elements of the direct sum with trivial sum (or product), in this case in  $\Gamma$ . (As we have not assumed that any  $v \in Q^+$  is inert in  $F_\infty^+$ , the left column need not be right exact.) This image is the Frobenius module  $M_Q$  of Khare-Wintenberger [KW, Definition 4.1].

By its definition, the  $\mathfrak{q}$ -ray class group  $\text{Cl}_{\infty, \mathfrak{q}}$  of  $F_\infty$  fits into an exact sequence

$$1 \rightarrow \mathcal{O}_{\infty, \mathfrak{q}}^\times \rightarrow \mathcal{O}_\infty^\times \rightarrow (\mathcal{O}_\infty/\mathfrak{q})^\times \rightarrow \text{Cl}_{\infty, \mathfrak{q}} \rightarrow \text{Cl}_\infty \rightarrow 0,$$

where  $\mathcal{O}_{\infty, \mathfrak{q}}^\times$  denotes the group of units in  $\mathcal{O}_\infty$  that are congruent to 1 modulo  $\mathfrak{q}$ . Since the minus part of  $\mathcal{O}_\infty^\times$  is its group of roots of unity, this gives rise to an exact sequence

$$0 \rightarrow \mu_{p^\infty}(F_\infty) \rightarrow \bigoplus_{u \in Q_\infty^+} \mu_{p^\infty}(F_{\infty, u}^+) \rightarrow A_{\infty, \mathfrak{q}}^- \rightarrow A_\infty^- \rightarrow 0 \tag{2.2}$$

on  $p$ -parts of minus parts, where the first map is the diagonal embedding.

Note that  $A_\infty^-$  is Kummer dual to  $\mathfrak{X}_\infty^+$ , which is to say dual via homomorphisms to  $\mu_{p^\infty}$ . Therefore, the Kummer dual of the exact sequence

$$0 \rightarrow \bigoplus'_{u \in Q_\infty^+} \mu_{p^\infty} \rightarrow A_{\infty, \mathfrak{q}}^- \rightarrow A_\infty^- \rightarrow 0 \tag{2.3}$$

induced by (2.2), where  $\bigoplus'$  denotes quotient by the diagonal, has the form

$$0 \rightarrow \mathfrak{X}_\infty^+ \rightarrow \text{Hom}(A_{\infty, \mathfrak{q}}^-, \mu_{p^\infty}) \rightarrow \bigoplus_{u \in Q_\infty^+}^0 \mathbf{Z}_p \rightarrow 0. \tag{2.4}$$

In  $\Gamma$ -homology, we have canonical isomorphisms  $H_1(\Gamma, \mathbf{Z}_p) \cong \Gamma$  and

$$H_1\left(\Gamma, \bigoplus_{\substack{u \in Q_\infty^+ \\ u|v}} \mathbf{Z}_p\right) \cong \left(\bigoplus_{\substack{u \in Q_\infty^+ \\ u|v}} \Gamma\right)^\Gamma \cong \Gamma_v$$

for each  $v \in Q^+$ , the last map being induced by multiplication in  $\Gamma$ . It follows that the connecting homomorphism in the  $\Gamma$ -homology of (2.4) has the form

$$\kappa^0: \bigoplus_{v \in Q^+}^0 \Gamma_v \rightarrow (\mathfrak{X}_\infty^+)_\Gamma.$$

With both  $\delta^0$  and  $\kappa^0$  canonically defined, it is reasonable to consider the following statement.

**Theorem 2.1.** *The map  $\kappa^0$  is equal to  $\delta^0$ .*

Before we proceed to the proof, let us compare Theorem 2.1 with the formulation of the reciprocity conjecture given in [KW] and the introduction. So, suppose that  $|Q_\infty^+| = 2$ . In this case, the image of  $\kappa^0$  is the ray class line  $N_Q$ . More precisely, Khare and Wintenberger consider the class  $\xi_Q$  of the exact sequence (2.3) in

$$\begin{aligned} H^1(\Gamma, \text{Hom}(A_\infty^-, (\mu_{p^\infty} \oplus \mu_{p^\infty})')) &\cong H^1(\Gamma, \text{Hom}(A_\infty^-, \mu_{p^\infty})) \\ &\cong H^1(\Gamma, \mathfrak{X}_\infty^+) \cong \text{Hom}(\Gamma, (\mathfrak{X}_\infty^+)_\Gamma), \end{aligned}$$

where the isomorphism  $(\mu_{p^\infty} \oplus \mu_{p^\infty})' \xrightarrow{\sim} \mu_{p^\infty}$  takes  $(\alpha, \beta)$  to  $\alpha\beta^{-1}$ , which requires a choice of one of the two primes in  $Q$ . They then evaluate  $\xi_Q$  on a noncanonical choice of generator of  $\Gamma$  and define  $N_Q$  to be the  $\mathbf{Z}_p$ -submodule it generates [KW, Section 5.1], which is independent of the choices made. We claim that  $\xi_Q$  is the negative of the class in  $\Gamma$ -cohomology of the dual sequence (2.4), which also lies in

$$H^1(\Gamma, \text{Hom}((\mathbf{Z}_p \oplus \mathbf{Z}_p)^0, \mathfrak{X}_\infty^+)) \cong H^1(\Gamma, \mathfrak{X}_\infty^+),$$

the isomorphism  $(\mathbf{Z}_p \oplus \mathbf{Z}_p)^0 \xrightarrow{\sim} \mathbf{Z}_p$  used here taking  $(a, -a)$  to  $a$ , with the first coordinate corresponding to the same prime of  $Q$  as before. The latter class as viewed in  $(\mathfrak{X}_\infty^+)_\Gamma$  agrees with  $\kappa^0$  evaluated on the chosen generator. Supposing the claim, since the  $\mathbf{Z}_p$ -span of the image of  $\delta^0$  is by definition the Frobenius line  $M_Q$ , we see that Theorem 2.1 implies the reciprocity conjecture. Moreover, in the notation of the introduction, we have  $m_Q = \delta^0(\varphi_1)$  and  $n_Q = -\kappa^0(\varphi_1)$ , so Theorem 2.1 implies Theorem 1.6 as well.

As for the claim, it follows easily from the following simple lemma.

**Lemma 2.2.** *The class in  $H^1(\Gamma, \text{Hom}(C, A))$  of an exact sequence of finitely generated  $\Lambda$ -modules*

$$0 \rightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \rightarrow 0$$

*is sent to the negative of the class in  $H^1(\Gamma, \text{Hom}(A^\vee, C^\vee))$  of the Pontryagin dual exact sequence under the isomorphism*

$$\text{Hom}(C, A) \xrightarrow{\sim} \text{Hom}(A^\vee, C^\vee), \quad f \mapsto f^\vee$$

*given by  $f^\vee(\phi) = \phi \circ f$  for  $f \in \text{Hom}(C, A)$  and  $\phi \in A^\vee$ .*

*Proof.* For any set-theoretic map  $\kappa: M \rightarrow N$  of  $\Lambda$ -modules and  $\gamma \in \Gamma$ , we define  $\kappa^\gamma: M \rightarrow N$  by  $\kappa^\gamma(m) = \gamma\kappa(\gamma^{-1}m)$  for each  $m \in M$ . For any continuous function  $s$  splitting  $\pi$ , the class of our exact sequence is that of the cocycle  $\chi$  given by  $\iota \circ \chi(\gamma) = s^\gamma - s$ . Let  $t: B \rightarrow A$  be the unique map satisfying  $\iota \circ t = 1 - s \circ \pi$ . The class of the Pontryagin dual sequence is that of the cocycle  $\chi^*: \Gamma \rightarrow \text{Hom}(A^\vee, C^\vee)$  given by

$$\pi^\vee(\chi^*(\gamma)(\phi)) = (t^\vee)^\gamma(\phi) - t^\vee(\phi) = \phi \circ (t^\gamma - t)$$

for  $\phi \in A^\vee$ . Taking the dual of  $\chi(\gamma)$  and noting that  $\iota \circ t^\gamma = 1 - s^\gamma \circ \pi$ , we obtain

$$\pi^\vee(\chi(\gamma)^\vee(\phi)) = \phi \circ \iota^{-1} \circ (s^\gamma - s) \circ \pi = \phi \circ (t - t^\gamma),$$

as desired. □

### 3 The proof

To begin with, note that the class group of the maximal  $p$ -ramified extension  $\Omega$  of  $F$  is trivial as  $\Omega$  contains the Hilbert class field of every number field in  $\Omega$ . Let us set

$$\mathcal{W} = \varinjlim_{E \subset \Omega} \bigoplus_{w \in Q_E} \mu_{p^\infty}(E_w),$$

where the direct limit runs over the number fields  $E$  containing  $F$  in  $\Omega$ . Note that  $\mathcal{W}$  is  $H$ -induced from  $\bigoplus_{Q_\infty} \mu_{p^\infty}$ , so

$$\mathcal{W}^H = \bigoplus_{u \in Q_\infty} \mu_{p^\infty}$$

and  $H^i(H, \mathcal{W}) = 0$  for  $i \geq 1$ . For any  $u \in Q_\infty^+$ , the  $u$ -component of  $\mathcal{W}^H$  will be  $\mu_{p^\infty}$  if the prime  $v$  below  $u$  is inert in  $F/F^+$ , and it will be  $\mu_{p^\infty} \oplus \mu_{p^\infty}$ , with complex conjugation



acting by switching coordinates, if the prime  $v$  splits in  $F/F^+$ . Either way, the minus part is  $\mu_{p^\infty}$ . Therefore, we have

$$(\mathcal{W}^H)^- = \bigoplus_{u \in Q_\infty^+} \mu_{p^\infty}.$$

Now set  $\omega = \mathcal{W}/\mu_{p^\infty}$  with respect to the diagonal embedding of  $\mu_{p^\infty}$ . We then obtain a long exact sequence in  $H$ -cohomology, the minus part of which begins

$$1 \rightarrow \mu_{p^\infty} \rightarrow \bigoplus_{u \in Q_\infty^+} \mu_{p^\infty} \rightarrow (\omega^H)^- \rightarrow A_\infty^- \rightarrow 0, \quad (3.1)$$

the term  $A_\infty^-$  being  $H^1(H, \mu_{p^\infty})^-$  by Kummer theory.

We make the following claim.

**Proposition 3.1.** *There is an isomorphism  $\phi: A_{\infty, \mathfrak{q}}^- \rightarrow (\omega^H)^-$  of  $\Lambda$ -modules fitting into an isomorphism of exact sequences of  $\Lambda$ -modules*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_{p^\infty} & \longrightarrow & \bigoplus_{Q_\infty^+} \mu_{p^\infty} & \longrightarrow & A_{\infty, \mathfrak{q}}^- & \longrightarrow & A_\infty^- \longrightarrow 0 \\ & & \parallel & & \parallel & & \downarrow \phi & & \parallel \\ 1 & \longrightarrow & \mu_{p^\infty} & \longrightarrow & \bigoplus_{Q_\infty^+} \mu_{p^\infty} & \longrightarrow & (\omega^H)^- & \longrightarrow & A_\infty^- \longrightarrow 0 \end{array}$$

from (2.2) to (3.1).

*Proof.* We define  $\phi$  explicitly. Let  $\mathfrak{a}$  be a nonzero finitely generated fractional ideal of  $\mathcal{O}_\infty$  that is relatively prime to  $p$  and the ideals in  $Q_\infty$ , and suppose that its ray class  $[\mathfrak{a}]_{\mathfrak{q}}$  lies in  $A_{\infty, \mathfrak{q}}^-$ . Let  $[\mathfrak{a}]$  denote its class in  $A_\infty^-$ . Let  $n$  be such that  $\mathfrak{a}^{p^n}$  is principal, therefore generated by some  $a \in F_\infty^\times$ . We assume, as is possible, that  $\mathfrak{a}$  and  $a$  are chosen so that  $s\mathfrak{a} = \mathfrak{a}^{-1}$  and  $s(a) = a^{-1}$ , where  $s$  denotes the generator of  $\text{Gal}(F_\infty/F_\infty^+)$ . Let  $\alpha$  be such that  $\alpha^{p^n} = a$ , and note that  $\alpha \in \Omega^\times$ , since  $\alpha$  generates a  $p$ -ramified extension of  $F_\infty$ . Since  $[\mathfrak{a}]_{\mathfrak{q}}$  has  $p$ -power order, we have  $a^{p^t} \equiv 1 \pmod{\mathfrak{q}_\infty}$  for sufficiently large  $t$ . Therefore, the image

$$\bar{\alpha} \in \varinjlim_{E \subset \Omega} (\mathcal{O}_E/\mathfrak{q}_E)^\times$$

of  $\alpha$  has  $p$ -power order, so it lies in the  $p$ -power torsion subgroup  $\mathcal{W}$  of the direct limit. For  $\sigma \in H$ , we have  $\bar{\alpha}^{\sigma-1} = \alpha^{\sigma-1} \in \mu_{p^n}$ , so the image  $\phi([\mathfrak{a}]_{\mathfrak{q}})$  of  $\bar{\alpha}$  in  $\omega$  lies in  $\omega^H$ .

Note that if  $\tau \in \text{Gal}(\Omega/F^+)$ , then the class  $\tau([\mathfrak{a}]_{\mathfrak{q}})$  is represented by  $\tau\mathfrak{a}$ , the  $p^n$ th power of which is generated by  $\tau(a)$ , and this has  $\tau(\alpha)$  as a  $p^n$ th root. This, in turn, has image  $\tau(\bar{\alpha})$  in  $\mathcal{W}$ . In particular, since  $[\mathfrak{a}]_{\mathfrak{q}}$  lies in the minus part of  $A_{\infty, \mathfrak{q}}$ , the element

$\phi([a]_q)$  lies in the minus part of  $\omega^H$ . Since  $\phi$  is multiplicative given consistent choices, if we can show that  $\phi([a]_q)$  is well-defined, we will then have constructed a homomorphism  $\phi$  of  $\Lambda$ -modules.

We show that  $\phi$  is well-defined. First, suppose that  $n$  is replaced by some  $m \geq n$  and  $a$  by  $a^{p^{m-n}}$ . Then  $\alpha$  can still be taken to be the same element. On the other hand, for a fixed  $n$ , we may replace  $\alpha$  by a product of it with a  $p^n$ th root of unity. However, this does not affect the image of  $\bar{\alpha}$  in  $\omega$ . Next, any generator of  $\mathfrak{a}^{p^n}$  in  $(F_\infty^\times)^-$  will differ from  $a$  by some element of the minus part  $\mu_{p^\infty}$  of  $\mathcal{O}_\infty^\times$ , the  $p^n$ th root of this element will be another  $p$ -power root of unity, and again this will not change the image of  $\bar{\alpha}$  in  $\omega$ . Finally, any finitely generated fractional ideal  $\mathfrak{b}$  prime to  $Q_\infty$  and  $p$  and representing the class  $[a]_q$  has the form  $\mathfrak{b} = \mathfrak{a}(c)$ , where  $c \in F_\infty^\times$  with  $c \equiv 1 \pmod{\mathfrak{q}_\infty}$ . Then  $\mathfrak{b}^{p^n}$  is generated by  $ac^{p^n}$ , which has  $p^n$ th root  $\alpha c$ . The image of this element in the direct limit of the groups  $(\mathcal{O}_E/\mathfrak{q}_E)^\times$  is just  $\bar{\alpha}$ . Having checked independence of all choices, we have that  $\phi$  is well-defined.

It remains only to check the commutativity of the diagram. For this, suppose that  $(\alpha_u)_u \in \bigoplus_{u \in Q_\infty^+} \mu_{p^\infty}$ , and let  $a \in \mathcal{O}_\infty$  with  $s(a) = a^{-1}$  be such that  $a$  has image  $\alpha_u$  in the residue field of  $\mathcal{O}_\infty$  for each of the one or two primes of  $Q_\infty$  lying over each  $u \in Q_\infty^+$ . Then the class  $[(a)]_q$  is represented by  $(a)$  and has image  $(\alpha_u)_u$  in  $\bigoplus_{u \in Q_\infty^+} \mu_{p^\infty}$  and therefore the image of that in  $\omega^H$ . Hence, the middle square commutes. As for the right-hand square, let  $[a]_q \in A_{\infty,q}^-$ , and note that  $\phi([a]_q)$  is the image of  $\bar{\alpha}$  as before. The connecting homomorphism  $\omega^H \rightarrow H^1(H, \mu_{p^\infty})$  then takes  $\phi([a]_q)$  to the cocycle  $\tau \mapsto \bar{\alpha}^{\tau-1}$  for  $\tau \in H$ , which as we have already mentioned is just the Kummer character  $\tau \mapsto \alpha^{\tau-1}$ . Since  $\mathfrak{a}^{p^n} = (a)$  and  $\alpha^{p^n} = a$ , this character has image  $[a]$  in  $A_\infty^-$ , as desired.  $\square$

Having shown that the class of

$$1 \rightarrow \bigoplus'_{u \in Q_\infty^+} \mu_{p^\infty} \rightarrow (\omega^H)^- \rightarrow A_\infty^- \rightarrow 0 \quad (3.2)$$

agrees with the class of (2.3), the first connecting homomorphism in the long exact sequence in the  $\Gamma$ -cohomology of (3.2) will now be the negative of the Pontryagin dual of  $\kappa^0$  (as follows from Lemma 2.2). In order to compare this with  $\delta^0$ , we will reconstruct the diagram (2.1) in a manner that incorporates the latter sequence.

Let us start by defining the needed object  $\mathcal{V}$ , which most simply put is just the twist  $\mathcal{W}(-1)$ . More meticulously, for each  $v \in Q$ , we can set

$$\mathcal{V}_v = \varinjlim_{E \subset \Omega} \bigoplus_{\substack{w \in Q_E \\ w|v}} \mathbb{Q}_p / \mathbb{Z}_p$$

and then take

$$\mathcal{V} = \bigoplus_{v \in Q} \mathcal{V}_v = \lim_{\substack{\rightarrow \\ E \subset \Omega}} \bigoplus_{w \in Q_E} \mathbf{Q}_p/\mathbf{Z}_p.$$

Let  $\nu$  be the quotient of  $\mathcal{V}$  by  $\mathbf{Q}_p/\mathbf{Z}_p$  embedded diagonally. As with  $\mathcal{W}$ , note that  $\mathcal{V}$  is the  $H$ -induced module of  $\bigoplus_{Q_\infty} \mathbf{Q}_p/\mathbf{Z}_p$  (in that  $\mathcal{W}$  is the Tate twist of  $\mathcal{V}$ ). Therefore, the long exact sequence in  $H$ -cohomology attached to

$$0 \rightarrow \mathbf{Q}_p/\mathbf{Z}_p \rightarrow \mathcal{V} \rightarrow \nu \rightarrow 0 \quad (3.3)$$

gives rise to a short exact sequence

$$0 \rightarrow \bigoplus_{u \in Q_\infty}' \mathbf{Q}_p/\mathbf{Z}_p \rightarrow \nu^H \rightarrow \mathfrak{X}_\infty^\vee \rightarrow 0. \quad (3.4)$$

There is a commutative diagram

$$\begin{array}{ccccccccccc} & & & & H^1(\Gamma, \mathcal{V}^H) & \rightarrow & H^1(\Gamma, \nu^H) & \longrightarrow & H^1(\Gamma, \mathfrak{X}_\infty^\vee) & \longrightarrow & 0 \\ & & & & \beta \downarrow \wr & & \theta \downarrow \wr & & \psi \downarrow \wr & & \\ 0 \rightarrow & \mathbf{Q}_p/\mathbf{Z}_p & \rightarrow & \mathcal{V}^G & \rightarrow & \nu^G & \rightarrow & H^1(G, \mathbf{Q}_p/\mathbf{Z}_p) & \rightarrow & H^1(G, \nu) & \rightarrow & H^2(G, \mathbf{Q}_p/\mathbf{Z}_p) & \rightarrow & 0 \end{array} \quad (3.5)$$

in which  $\beta$  and  $\theta$  are inflation maps, the lower row is the long exact sequence in  $G$ -cohomology arising from (3.3), and  $\psi$  is the unique map making the diagram commute. The right exact top row is induced on  $\Gamma$ -cohomology by the right exact sequence

$$\mathcal{V}^H \rightarrow \nu^H \rightarrow \mathfrak{X}_\infty^\vee \rightarrow 0$$

giving rise to (3.4), noting that  $\Gamma$  has cohomological dimension 1. The surjectivity of  $\beta$  follows from the inflation-restriction sequence and the fact that  $H^1(H, \mathcal{V}) = 0$ . Similarly, the cokernel of  $\theta$  injects into  $H^1(H, \nu) \cong H^2(H, \mathbf{Q}_p/\mathbf{Z}_p)$ , and the latter group is trivial by weak Leopoldt ([I2], but see [NSW, Theorem 10.3.22] for this form). The interested reader may check that  $\psi$  arises as the map  $E_2^{1,1} \rightarrow E^2$  (noting that  $E_2^{i,j} = 0$  for  $i \geq 2$ ) in the Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i(\Gamma, H^j(H, \mathbf{Q}_p/\mathbf{Z}_p)) \Rightarrow E^{i+j} = H^{i+j}(G, \mathbf{Q}_p/\mathbf{Z}_p),$$

(i.e., there is a morphism from the corresponding spectral sequence with  $\nu$  coefficients to this sequence with a shift of degree).

Replacing the last three terms in the bottom row of (3.5) using the isomorphisms with the terms of the top row and mapping the resulting exact sequence to the long

exact sequence in  $\Gamma$ -cohomology attached to (3.4), we obtain a diagram

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \bigoplus_Q' \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & \nu^G & \longrightarrow & \mathfrak{X}^\vee & \xrightarrow{\iota} & H^1(\Gamma, \bigoplus_{Q_\infty} \mathbf{Q}_p/\mathbf{Z}_p) & \rightarrow & H^1(\Gamma, \nu^H) & \rightarrow & H^1(\Gamma, \mathfrak{X}_\infty^\vee) & \rightarrow & 0 \\
& & \downarrow & & \parallel & & \downarrow \text{Res} & & \downarrow -\pi & & \parallel & & \parallel & & \\
0 & \rightarrow & (\bigoplus_{Q_\infty}' \mathbf{Q}_p/\mathbf{Z}_p)^\Gamma & \rightarrow & \nu^G & \rightarrow & (\mathfrak{X}_\infty^\vee)^\Gamma & \xrightarrow{\partial} & H^1(\Gamma, \bigoplus_{Q_\infty}' \mathbf{Q}_p/\mathbf{Z}_p) & \rightarrow & H^1(\Gamma, \nu^H) & \rightarrow & H^1(\Gamma, \mathfrak{X}_\infty^\vee) & \rightarrow & 0.
\end{array} \tag{3.6}$$

Here, the map Res is restriction on homomorphism groups, and the map  $\pi$  is induced by the quotient map

$$\bigoplus_{u \in Q_\infty} \mathbf{Q}_p/\mathbf{Z}_p \rightarrow \bigoplus_{u \in Q_\infty}' \mathbf{Q}_p/\mathbf{Z}_p.$$

Clearly, Res has kernel  $\Gamma^\vee$  and  $\pi$  has kernel an infinite quotient of  $\Gamma^\vee$ . However, it is not immediately clear that the middle square in the diagram commutes, so we prove this.

**Proposition 3.2.** *The diagram (3.6) is commutative.*

*Proof.* The only square for which commutativity is nonobvious is the third, so we focus on it. Let  $\chi \in G^\vee = \mathfrak{X}^\vee$ , and restrict  $\chi$  to  $H$  (so, to an element of  $(\mathfrak{X}_\infty^\vee)^\Gamma$ ). Find  $a \in \mathcal{V}$  such that the image  $\bar{a}$  of  $a$  in  $\nu$  is fixed by  $H$  and maps to  $\chi|_H$  under the natural map  $\nu^H \rightarrow \mathfrak{X}_\infty^\vee$ . That is,  $\chi(\tau) = (\tau - 1)a$  for all  $\tau \in H$ . Then  $\partial(\chi|_H)$  is the unique homomorphism such that

$$\partial(\chi|_H)(\gamma) = (\tilde{\gamma} - 1)\bar{a}$$

for every  $\gamma \in \Gamma$  and any lift of it to  $\tilde{\gamma} \in G$ . This homomorphism takes values in  $\bigoplus_{Q_\infty}' \mathbf{Q}_p/\mathbf{Z}_p$  inside  $\nu^H$ , since  $\chi|_H$  is fixed by  $\Gamma$ .

On the other hand, we may view  $\chi$  as an element of  $H^1(G, \mathcal{V})$  via the diagonal embedding of  $\mathbf{Q}_p/\mathbf{Z}_p$  in  $\mathcal{V}$ . Since  $\chi(\tau) = (\tau - 1)a$  for  $\tau \in H$ , its image  $\iota(\chi)$  in  $H^1(\Gamma, \bigoplus_{Q_\infty} \mathbf{Q}_p/\mathbf{Z}_p)$  under the inverse of inflation is represented by a cocycle given by

$$\iota(\chi)(\gamma) = \chi(\tilde{\gamma}) - (\tilde{\gamma} - 1)a \tag{3.7}$$

for  $\gamma \in \Gamma$ , viewing  $\bigoplus_{Q_\infty} \mathbf{Q}_p/\mathbf{Z}_p$  as  $\mathcal{V}^H$ . We then have

$$\pi(\iota(\chi))(\gamma) = -(\tilde{\gamma} - 1)\bar{a}$$

since  $\chi(\gamma) \in \mathbf{Q}_p/\mathbf{Z}_p$ , so  $\pi \circ \iota = -\partial \circ \text{Res}$ , as claimed.  $\square$

We now define

$$\kappa^0: \bigoplus_{v \in Q^+}^0 \Gamma_v \rightarrow (\mathfrak{X}_\infty^+)_\Gamma$$

to be the negative of the plus part of the Pontryagin dual of the connecting homomorphism  $\partial$  and

$$\kappa: \bigoplus_{v \in Q^+} \Gamma_v \rightarrow \mathfrak{X}^+$$

to be the plus part of the Pontryagin dual of the map  $\iota$  found in (3.6). This definition of  $\kappa^0$  agrees with that Section 2. The plus part of the Pontryagin dual of the third commutative square in (3.6) then yields the commutative square

$$\begin{array}{ccc} \bigoplus_{v \in Q^+}^0 \Gamma_v & \xrightarrow{\kappa^0} & (\mathfrak{X}_\infty^+)_\Gamma \\ \downarrow & & \downarrow \\ \bigoplus_{v \in Q^+} \Gamma_v & \xrightarrow{\kappa} & \mathfrak{X}^+, \end{array} \quad (3.8)$$

in which the right and left vertical maps are the canonical injections with cokernel  $\Gamma$  and contained in  $\Gamma$ , respectively. In the proof of the following, which implies Theorem 2.1, we shall see that  $\kappa = \delta$  and therefore  $\kappa^0 = \delta^0$ , so the diagram (3.8) agrees with (2.1).

We may now prove our main theorem.

*Proof of Theorem 2.1.* By the commutativity of (3.8), we need only show that  $\kappa$  is the map  $\delta$  of the introduction. Note that we have already described a map  $\iota$  in the proof of Proposition 3.2, the plus part of which may be identified with the Pontryagin dual of  $\kappa$ . So, we consider the plus part

$$\iota^+: (\mathfrak{X}^+)^\vee \rightarrow H^1\left(\Gamma, \bigoplus_{u \in Q_\infty^+} \mathbf{Q}_p/\mathbf{Z}_p\right)$$

of  $\iota$ . The map  $\iota^+$  may be viewed as a collection of maps  $\iota_v^+: (\mathfrak{X}^+)^\vee \rightarrow \Gamma_v^\vee$  for each  $v \in Q^+$  via the isomorphism

$$H^1\left(\Gamma, \bigoplus_{\substack{u \in Q_\infty^+ \\ u|v}} \mathbf{Q}_p/\mathbf{Z}_p\right) \xrightarrow{\sim} \text{Hom}(\Gamma_v, \mathbf{Q}_p/\mathbf{Z}_p)$$

that takes a cocycle  $f$  to its restriction to  $\Gamma_v$ , which has values in the diagonal  $\mathbf{Q}_p/\mathbf{Z}_p$  in the direct sum.

By (3.7), for  $\chi \in (\mathfrak{X}^+)^\vee$ , which we may think of as an element of  $G^\vee$ , and  $\gamma_v \in \Gamma_v$ , we may write

$$\iota_v^+(\chi)(\gamma_v) = \chi(\tilde{\gamma}_v) - (\tilde{\gamma}_v - 1)a_v.$$

for some lift  $\tilde{\gamma}_v$  of  $\gamma_v$  in  $G$  and  $a_v \in \mathcal{V}_v$ . By definition of  $\mathcal{V}_v$ , there exists a number field  $E$  containing  $F$  such that  $a_v$  lies in the direct sum  $\bigoplus_{w|v} \mathbf{Q}_p/\mathbf{Z}_p$  over primes  $w$  of  $E$  lying over  $v$ , and  $\tilde{\gamma}_v$  acts on the sum by permuting the coordinates of its elements. In particular, the  $w$ -coordinate of  $\iota_v^+(\chi)(\gamma_v)$  in this direct sum is

$$\chi(\tilde{\gamma}_v) - (a_v)_{\tilde{\gamma}_v^{-1}(w)} + (a_v)_w.$$

If we pick  $\tilde{\gamma}_v$  to lie in the decomposition group of  $G$  at a place over  $w$ , then the  $w$ -coordinate of  $\iota_v^+(\chi)(\gamma_v)$  will equal  $\chi(\tilde{\gamma}_v)$ , but then every  $w$ -coordinate for  $w$  lying over  $v$  must have this value since  $\iota_v^+(\chi)$  takes values on  $\Gamma_v$  in the diagonally embedded  $\mathbf{Q}_p/\mathbf{Z}_p$  in  $\mathcal{V}_v$ . As  $\tilde{\gamma}_v$  will restrict to an element of the decomposition group  $D_v$  in  $\mathfrak{X}^+$ , the  $v$ -component  $\delta_v$  of  $\delta$  satisfies

$$\delta_v^\vee(\chi)(\gamma_v) = \chi(\tilde{\gamma}_v) = \iota_v^+(\chi)(\gamma_v).$$

For the sums of the Pontryagin duals, this says exactly that  $\kappa = \delta$ . □

## References

- [I1] K. Iwasawa, On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan* **16** (1964), 42–82.
- [I2] K. Iwasawa, On  $\mathbf{Z}_l$ -extensions of algebraic number fields, *Ann. of Math.* **98** (1973), 246–326.
- [KW] C. Khare, J.-P. Wintenberger, Ramification in Iwasawa modules, preprint, arXiv:1101.6393.
- [L] H.-W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, *J. Reine Angew. Math.* **209** (1962), 54–71.
- [NSW] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, 2nd ed., Grundlehren Math. Wiss. **323**, Springer, 2008.